中山醫學大學

資通安全管理政策

機密等級：一般

文件編號：IS-A-001

版　　次：3.0

發行日期：112.04.24

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	97.10.24		張巧蓉	初版
1.1	99.12.07		張巧蓉	增訂 3.1 高階管理者目標
1.2	102.07.24	2 至 4	張巧蓉	增訂『第五節 管理指標』擬訂『5.1 定量化指標』與『5.2 定性化指標』
1.3	103.04.22	2 至 3	張巧蓉	修訂『5.1 定量化指標』5.1.2 及 5.1.5
1.4	104.08.24	3 至 4	張巧蓉	因應 104 學年組織變動，修訂 5.2.1、5.2.3、5.2.6 項之下的『本中心』為『圖書資訊處』
1.5	105.10.25	3	趙慧婷	修訂『5.1 定量化指標』5.1.4 及 5.1.6
2.0	107.06.07		趙慧婷	轉版
2.1	107.12.05	2	趙慧婷	修訂 5.1.4
2.2	108.08.01	1、4	趙慧婷	因應委員會設置辦法修訂，「資訊安全委員會」修改為「中山醫學大學資訊安全暨個人資料保護委員會」
2.3	109.08.17	封面	趙慧婷	校徽更換
3.0	112.04.24	封面、 1 至 4	林翊樺	1. 配合組織辦法「中山醫學大學資訊安全暨個人資料保護委員會」，變更為「中山醫學大學資通安全管理委員會」調整修訂。 2. 配合資通安全導入全校，進行改版。 3. 1、3.4、5.3.1 加入適法性與相關法令。 4. 配合資安法修訂 5.1.3~5.1.5。 5. 增加 5.3.7，導入 PDCA 精神。 6. 增加 7.2，本政策實施時應予以公告。

資通安全管理政策					
文件編號	IS-A-001	機密等級	一般	版次	3.0

目錄

資通安全管理政策					
文件編號	IS-A-001	機密等級	一般	版次	3.0

1 目的

本政策規範中山醫學大學（以下簡稱本校）資通安全管理制度，以確保本校管轄資訊資產之機密性、完整性、可用性及適法性，進而保障本校人員之權益。

2 適用範圍

本校人員、接觸本校業務資料之外機關人員、提供委外服務之廠商人員及訪客。

3 名詞定義

3.1 機密性（Confidentiality）：使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

3.2 完整性（Integrity）：保護資產的準確度（Accuracy）和完全性（Completeness）的性質。

3.3 可用性（Availability）；經授權個體因應需求之可存取及可使用的性質。

3.4 適法性(Legality) ：符合國家相關法令規範。

3.5 資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

3.6 資訊資產：凡本校作業流程中使用之資訊資產，如內外部人員、紙本文件、電子文件、網路服務、電腦應用軟體、應用系統、電腦硬體、網路設備、環控系統、建築保護設施與便利設施等皆屬之。

4 權責

設置本校「中山醫學大學資通安全管理委員會」，負責政策之核定及監督、資通安全預防及危機處理。

5 要求事項

5.1 資通安全目標

5.1.1 本校每年無發生教職員生機密級資料外洩。

5.1.2 本校每年無發生教職員生資料(如:學生成績或使用者個人資料)遭竄改。

5.1.3 確保本校核心業務系統資訊機房維運服務達全年上班時間 95%以上之可用性，並確保維運服務中斷之情事，每次最長不得超過 8 小時。

5.1.4 本校核心業務系統服務達全年上班時間 95%以上之可用性，因資通安全事件、異常事件、其他安全事件造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 24 小時。

5.1.5 因資通安全事件、異常事件、其他安全事件造成系統、主機異常而中斷營運服務之情事，逾時通報案件每年不得超過 6 次。

5.2 資通安全管理事項

避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校帶來各種可能之風險及危害。資通安全管理涵蓋 14 項管理事項：

(1) 資通安全管理政策。

(2) 資通安全組織。

(3) 人力資源安全。

(4) 資產管理。

(5) 存取控制。

(6) 密碼學(加密控制) 。

(7) 實體與環境安全。

(8) 運作安全。

(9) 通訊安全。

(10) 系統取得、開發及維護。

(11) 供應者關係。

(12) 資通安全事件管理。

(13) 營運持續管理之資通安全層面。

(14) 遵循性。

5.3 資通安全管理原則

5.3.1 本校資通安全規範必須遵守政府相關法規（如：刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法、資通安全管理法及相關子法等）之規定。

5.3.2 重要之資訊資產應定期清查、分類分級與進行風險評鑑，並據以實施適當的防護措施。

5.3.3 重要資訊資產存取權限應予以區分，考量人員職務授予相關權限，必要時得採行加解密及身分鑑別機制，以加強資訊資產之安全。

5.3.4 對於資通安全事件須有完整的通報及應變措施，以確保資通系統、業務的持續運作。

5.3.5 應訂定營運持續計畫並定期演練，以確保重要系統、業務於資通安全事件發生時能於預定時間內恢復作業。

5.3.6 相關人員應依規定接受資通安全教育訓練與宣導，以加強資通安全認知。

5.3.7 定期辦理資通安全內部稽核活動及召開管理審查會議，透過不斷持續改善的過程，亦即 PDCA（計畫、執行、稽核、改善）精神，確保資通安全管理系統實施之有效性。

5.3.8 違反本政策與資通安全相關規範，依相關法規或本校懲戒規定辦理。

5.3.9 本政策依業務變動、技術發展及風險評鑑的結果修訂。

6 審查

本政策應至少每年審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本校永續運作及提供學術網路服務之能力。

7 實施

7.1 本政策經「中山醫學大學資通安全管理委員會」核定後實施，修訂時亦同。

7.2 本政策應以書面、電子（E-MAIL、網頁公告）或其他方式通知本校人員及接觸本校業務之公私機關（構）、往來廠商等關注方共同遵行。